(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/77790 A1

(51) International Patent Classification⁷: G06F 1/00, G07F 17/16

(21) International Application Number: PCT/EP01/04088

(22) International Filing Date: 10 April 2001 (10.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00401007.0 11 April 2000 (11.04.2000) EP

(71) Applicant *(for all designated States except US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DIEHL, Eric [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). FISCHER, Pierre [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Agent: BONNANS, Arnaud; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

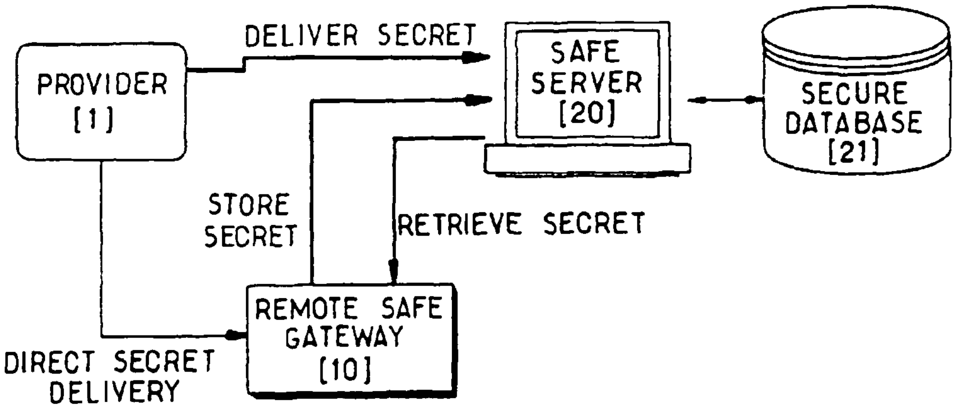
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT



(57) Abstract: A system for securely storing secret information comprises an apparatus (10; 1) containing the secret information, a device meant to use said secret information to decrypt a digital content and a remote server (20). The apparatus can send the secret information to the server (20) that has means for storing the secret information. A process with the following steps is proposed: initiating a remote communication between the apparatus (10; 1) and the remote server (20); sending the secret information from the apparatus (10; 1) to the server (20); storing the secret information on the server (20). A method for distribution of a digital content is also described.

SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT

Field of the invention

The invention relates generally to secure storage of secret information and more particularly to a system and a process for securely storing secret information and to an apparatus and a server to be used in said system. The invention also relates to a method for distribution of a digital content.

Background art

With the advent of digital TV, and copy protection, the access to content will be protected by rights. These rights may have many forms like entitlements, or dedicated decryption keys. The notion of rights might be extended to any secret information. All these type of data have in common that they need to be stored in a safe place.

Today none of the consumer devices has such tamper proof place. The price would be prohibitive. Only smart cards offer sufficient security. Unfortunately the size of memory of smart cards, and thus their storage capability, is limited. Furthermore a smart card can break down, or be lost. So today, once the user mislays his secret data, he will have no simple way to retrieve them. If these data represent user's rights acquired on digital content (for example the right to view a film or to listen to music) it may be prejudicial to the user if he loses these rights he has paid for.

Summary of the invention

The present invention is therefore directed to the problem of finding a way of safely and securely storing secret data to be used by a single device or by a device in a network. Another problem to be solved by the invention is to find a way of retrieving these secret data if the device or the network has lost them.

The invention relates to a system for securely storing secret information to be used by a device wherein said secret information is stored in a remote server. The device may be part of a home network and preferably the secret information is used by said device to access to a digital content.

Therefore, the remote server acts as a bank which maintains in a safe place digital secrets.

The invention proposes an apparatus containing secret information to be used by a device to decrypt a digital content and having means for sending said secret information to a remote server in order to store said information in said remote server, said server being remote from said device.

The invention also proposes a system for securely storing secret information comprising an apparatus containing said secret information, a device meant to use said secret information to decrypt a digital content and a server remote from said apparatus and from said device, wherein said apparatus comprises means for sending said secret information to said server and wherein said server comprises means for storing said secret information.

The apparatus may be part of said device, or may belong to the same home network as said device. In such cases, the apparatus is thereafter called the remote safe gateway. The apparatus may alternatively belong to a local network generating said secret information (*i.e.* belong to the secret provider).

According to another aspect of the invention, a server for securely storing secret information to be used by a device remote from said server to decrypt a digital content has means for receiving said secret information through a remote communication

A process is proposed for securely storing secret information to be used by a device to decrypt a digital content : this process comprises the steps of :

- initiating a remote communication between an apparatus containing said secret information and a server remote from said device ;
- sending said secret information from said apparatus to said server ;
- storing said secret information on said server.

The invention also relates to a method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server remote from said device for storing said secret information on said server ;
- providing means for said device to retrieve said secret information from said server and to decrypt the encrypted digital content with said secret information.

Brief description of the drawings

Fig. 1 illustrates the general architecture of a system according to the invention.

Fig. 2 illustrates the architecture of a device used in the system of Fig. 1.

Fig. 3 illustrates a process for storing secret information according to a first embodiment of the invention.

Fig. 4 illustrates a process for retrieving a secret information stored according to the process illustrated in Fig. 3.

Fig. 5 illustrates a second embodiment of the invention.

Fig. 6 illustrates a process for storing a secret information in the second embodiment of the invention.

Description of the preferred embodiments

In Fig. 1, we have illustrated a first embodiment of a system according to the invention. In this embodiment, the user has a Set Top Box device 10 (STB) with a return channel such as a PSTN (for "Public Switched Telephone Network") modem or a cable modem.

We assume that all the information to store securely can be carried to this STB. For instance, we can envisage that a complete home network can benefit from the remote safe facility. In this case, preferably, a unique device of the network will be able to store and retrieve secret information according to the invention. This unique dedicated STB is used as an apparatus called the remote safe gateway. Obviously it could be another type of device, for example a computer.

Through its return channel, each remote safe gateway interacts with a remote server 20 called the remote safe server. The remote server has direct access to its own secure database 21. The secure database will store safely and securely the secret information.

In a preferred embodiment of the system, the secure database will be duplicated at least once in different locations. This will avoid loss of data due to natural or malicious crashes. Nevertheless, only one occurrence of the secure database will be considered in the following in order to simplify the presentation of the invention.

The user receives his secrets from a secret provider 1 which is consider here as having generated the secret information. It may be for example a content provider which provides, with an encrypted content, a secret to decrypt this content.

The secret provider 1 provides the information directly to the remote safe gateway 10. The user may receive information from many secret providers.

The characteristics of the system are as follows :

- A user must be identified uniquely. It must not be possible to impersonate him.

- A user must be able to transfer the secret digital information stored in his home system to the safe server 20. No information must leak from this transfer. For that purpose, the remote safe gateway 10 is used to make this transfer.

- The user must be able to retrieve one, part, or all the information stored in his remote safe. No information must leak from this transaction. For that purpose, the remote safe gateway 10 is also used for this transaction.

- There must be no constraint on the format of the stored information.

We will now describe how the system is working.

A first stage of the process consists in the registration of the user. Prior to use the remote safe, the user must sign on the remote safe server's operator. For that purpose, he provides a set of personal information. The definition of these data depends on the operator and is out of the scope of this invention. In return the operator returns a set of secret user identity information (SI_{user}) used in the next stages. Among this set of information is the unique identifier (ID_{user}) that thoroughly defines a given user.

The channel used for this communication can be different from the return channel of the remote safe gateway. In any case the transfer of the secret user identity information (SI_{user}) needs to be secured. There are several possible ways: mailing of a smart card, encrypted information sent through the return channel, ... In the last case, the decryption key is transferred through a secure separate channel such as phone or post mail.

A second stage of the process consists in the storage of secret information in the safe. This requires several steps.

In a first step, the remote safe gateway authenticates the remote safe server using known authentication methods. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the storage operation fails.

In a third step, they define a common session key $K_{session}$. This means a remote communication is initiated between the remote safe server and the remote safe gateway.

Then, in a fourth step, the remote safe server creates a unique identifier, $InfID_{user\_i}$ for the information i to be stored. InfIDuser_i is unique for each information stored by the user. Its choice is fully under the control of the remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule *f*, so that $f(InfID_{user\_i}, ID_{user})=true$.

In a fifth step, the remote safe gateway sends the information i to store to the remote safe server. The information i is encrypted using the session key Ksession before being sent. In an optional step, the remote safe gateway encrypts the information i using a secret key of the remote safe gateway before using the session key. Thus, with this optional step, the remote safe server will not have access to the plain text information.

Then, in the last step, the remote safe server decrypts the received information using the session key Ksession and stores it into its secure database.

The transfer may be secured against transmission errors, or message tampering. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

A third stage of the process consists in the retrieval of the secret information from the remote safe server. This operation requires the following steps.

In a first step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the retrieval operation fails.

In a second step, they define a common session key Ksession.

Then, in a third step, the remote safe gateway provides the remote safe server with the unique identifier of the information to retrieve InfIDuser_i.

In a fourth step, the remote safe server checks the validity of InfIDuser_i. It checks if the corresponding information exists in the database and if this is the case, the remote safe server sends back the requested information to the requesting remote safe gateway in a fifth step. The information is encrypted using the session key Ksession before being sent to the remote safe gateway.

Then, in a last step, the remote safe gateway decrypts the received message using the session key Ksession.

Preferably, the transfer is secured against transmission errors, or message tampering. In that case, the remote safe gateway checks the integrity of the decrypted message before using it.

According to one preferred aspect of the invention, all the operations, except the registration phase, should be transparent to the user. In other words, the retrieval of the stored secrets should be automatic and should not request any interaction from the user.

Fig. 2 illustrates a possible architecture for the remote safe gateway. In this figure, only the elements which are necessary for the understanding of the invention have been represented.

The remote safe gateway has a Central Processing Unit (CPU) 100. It is assumed that the CPU has its own volatile memory and non-volatile memory where its program is stored. In addition, the remote safe gateway has a non-volatile memory space 101 called the identifiers' memory. The CPU 100 can read and write the content of this space.

The remote safe gateway has also a secure processor 102. This secure processor is a tamper proof device that has at least a dedicated CPU 110, a non volatile memory 111 (ROM – Read Only Memory) to store program and persistent data, a volatile memory 112 (RAM – Random Access Memory), and a dedicated non-volatile memory area 113, called the secret cache memory. The secure processor 102 is, in a preferred embodiment, a smart card.

The CPU 100 never handles actual secrets. It handles only information identifiers InfIDuser_i. It maintains a list of the secret information through a list of their corresponding InfIDuser_i. This list is stored in the identifiers' memory. This space needs not to be tamper-proofed. Therefore it is not costly. The size of the identifiers' memory should be chosen to be large enough to store the expected amount of information identifiers.

The secure processor's CPU 110 handles the actual secrets. It stores them in its secret cache memory 113. Unfortunately this space is limited in size due to cost. Therefore it will employ memory-caching techniques that optimize the use of the space. It will store the most recently used secrets and some of the most frequently used secrets.

If the remote safe gateway needs a secret information which is not readily available in the secret cache memory 113, then the secure processor's CPU 110 requests it to the remote safe server.

In one embodiment of the invention, the remote safe gateway is part of a digital home network where other devices are connected. Some of these devices can also handle secrets. In that case they may reproduce the architecture of Fig. 2. Nevertheless, only the remote safe gateway is able to communicate with the remote safe server. The other devices exchange, through secure communication, with the remote safe gateway their secrets to store or to retrieve.

We will now enter into more details of this first embodiment.

Registration of the user.

When signing on, the user receives the secret user identity information as follows:

- A unique identifier IDuser.

- A pair of public (PUB_{user}) and private (PRI_{user}) keys; the remote safe server encrypts with a public key cryptosystem that we will call CS1. RSA (Rivest-Shamir-Adleman public key cryptosystem) could be such a system.

- A public key certificate $CERT_{user}$ signed by the remote safe server using its private signature key PRI_{safe_sign}. The remote safe server signs with a public key cryptosystem that we will call CS2. RSA could be such a system. CS2 can be identical to CS1.

- The public key of the remote safe server PUB_{safe_enc} using cryptosystem CS1.

These data must be transferred safely to the user. It is especially important that his private key, $PRI_{user,}$ is kept secret. He may for example receive these data in a smart card sent to him via mail.

Storage of the secret information.

The format of the message to store is preferably defined as follows:

```
Info_To_Store = {
     InfIDuser_i
     Length_clear_text
     Clear_Text
     Length_secret
     for I=0 to Length_secret-1
          Secret_data[i]
     Checksum
}
```

where :

- InfIDuser_i is a unique identifier of the information stored by the user. This identifier is unique to the user and delivered by the safe server ;

- Clear_Text is an ASCII text that describes the stored secret information. Its content is user defined. It could be envisaged that the secret provider delivers a default value for this secret ;

- Length_clear_text defines the length in bytes of Clear_Text ;

- Secret_data is the secret to store in the remote safe ;

- Length_secret defines the length in bytes of Secret_data ;

- Checksum is the sum of all previous bytes of the packet.

The process for storing a secret information is illustrated in Fig. 3 and explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe server defines a new value for the information identifier, InfIDuser_i. It sends it to the remote safe gateway.

The remote safe gateway builds the message Info_To_Store with its secret data and InfIDuser_i. It encrypts it with the Triple DES algorithm using the common session key Ksession. It sends the encrypted message to the remote safe server that decrypts it using the common key Ksession.

The remote safe server checks the validity of Checksum. If the received message is valid, the remote safe server sends it to the secure database. If the operation was successful, the remote safe server returns an acknowledgement to the remote safe gateway, else it returns a non-acknowledgement.

Retrieving the secret information.

The process for retrieving a secret information stored in the remote safe server is illustrated by Fig. 4 and will be explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe gateway sends the reference of the data to retrieve: InfIDuser_i.

On receipt of the information identifier InfIDuser_i, the remote safe server passes it to the secure database.

The secure database checks if the message exists, i.e., if there is an information, own by the user, that has the right identification. If it is the case, then it returns the requested information Info_To_Retrieve to the remote safe server. The remote safe server encrypts the received data using Triple DES with the session key Ksession and It sends the encrypted message to the remote safe gateway.

The remote safe gateway decrypts the received message using the session key Ksession. It checks the validity of Checksum and if it is valid, the remote safe gateway uses the retrieved secret information Info_To_Retrieve.

We will now describe a second embodiment of the invention which is illustrated in Fig. 5.

In this embodiment, the secret provider can provide the information directly to the remote safe gateway or by an indirect way using the remote safe server. The user may receive information from many secret providers.

The additional characteristics of the system are as follows:

- A third party, known as the secret provider, can deposit a secret to the remote safe server on behalf of a user. No information must leak from this transaction.
- It is not possible to impersonate a secret provider.
- Once a secret as been deposited by a secret provider, the secret provider has no possible access to it.
- A secret provider cannot retrieve any information stored on the account of a user.
- Only an authorized secret provider can deposit a secret onto the account of a user.

In this embodiment, the process for the secret provider has two stages :

The first stage consists in the registration of the secret provider. As for the remote safe gateway, the secret provider needs to sign on the remote safe server. He signs on as secret provider. In return, it receives a set of information known as secret provider identity information (SI_{prov}).

The second stage consists in the storage of a secret information on behalf of a user. This stage requires several steps.

In a first step, the secret provider, through an apparatus of a local network of its own, authenticates the remote safe server. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the secret provider. If the authentication fails, then the storage operation fails.

In a third step, the remote safe server and the secret provider's apparatus define a common session key $K_{session.}$

Then, in a fourth step, the secret provider provides the identity of the user that he is acting for: ID_{user}.

In a fifth step, the remote safe server creates a unique identifier, InfIDuser_i for the information to be stored. InfIDuser_i is unique for each information stored by the user identified by IDuser. Its choice is fully under the control of the remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule.

In a sixth step, the secret provider sends the information to store to the remote safe server. The sent information is encrypted using the session key $K_{session}$.

In a last step, the remote safe server decrypts the received information using the session key $K_{session}$ and stores it into its secure database. The transfer may be secured against transmission errors, or message tampering using known techniques. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

Once the operation was successfully ended, then the secret provider sends the information identifier InfIDuser_i to the corresponding remote safe gateway. The secret provider does not keep any copy of it. Therefore, it is impossible for the secret provider to access any more to the secret information to retrieve it or to modify it.

Details of this second embodiment are explained bellow:

Registration of the secret provider

When signing on, the secret provider receives the following secret provider identity information:

- A unique identifier ID_{prov}.

- A pair of public (PUB_{prov}) and private (PRI_{prov}) keys; the remote safe server encrypts with the public key cryptosystem CS1.

- A public key certificate $CERT_{prov}$ signed by the remote safe server using its private signature key $PRI_{safe\_sign\_2}$; the safe server signs with the public key cryptosystem CS2.

- The public key of the remote safe server PUB_{safe_enc}.

These information must be transferred safely to the secret provider. It is especially important that his private key is kept secret

Storage of an information on behalf of a user.

This process, which is illustrated in Fig. 6, is similar to the process described previously in view of Fig. 3. The main differences are:

- Prior to exchange the secret information, the secret provider has to identify the user to whom is it depositing. The identification uses the user's unique identifier IDuser.

- Once the secret provider successfully stored the information, it sends the reference of the information to the user, that is to its remote safe gateway.

The system if the invention may be applied to a new distribution model. For example, a content provider wants to distribute in a controlled manner a content. This content can be any digital content such as video, MP3 files, software, etc. For that purpose it distributes the content encrypted with an encryption key $K_{enc\_cont\_i}$. To read this encrypted content, the user must have access to the decryption key $K_{dec\_cont\_i}$. The decryption key may be equal to the encryption if we use a symmetric cryptosystem. The user contacts the content provider and buys the right to access the content. Acting as a secret provider, the content provider deposits the decryption key in the user's remote safe. In return the user receives the information identifier of the decryption key.

Another possible application of the system of the invention is a small footprint backup of a jukebox. The jukebox will be a future new type of consumer device. It will probably be successful. Nevertheless with the jukebox, a major risk is introduced: loss of all the contents stored in the jukebox. Currently it is envisaged to use hard disks as storage units. In the field of software, it is well known that regular backup of the hard disk is a safe practice. But it is not reasonable to expect the same feature in a consumer device.

The system of the invention will provide a backup facility based on the remote safe as a new service. For each legally delivered content, the content provider will provide an additional information called a digital purchase proof. The digital purchase proof is the result of a one way cryptographic function using as input parameter a unique identifier of the owned content, and the user identifier ID_{user}. Instead of backing up all his contents, the user stores in his remote safe all his digital purchase proofs. If he loses one content, the user returns to the content provider the corresponding digital proof. The content provider checks if the digital proof is consistent with the claimed content and the identity of the user. If it is the case, then the content provider sends back to the user a copy of the content.

In conclusion, the invention offers the following advantages:

- the possibility to handle in a safe and secure manner a large quantity of secret data without requesting an in-house large tamper-proof space;

- a simple new model of distribution of digital content that could fit for IP streaming, or even prerecorded contents;

- a small size backup of large library of digital contents.

CLAIMS

1. Apparatus containing secret information to be used by a device to decrypt a digital content,

characterised by means for sending said secret information to a remote server (20) in order to store said information in said remote server (20), said server (20) being remote from said device.

2. Apparatus according to claim 1, being part of said device.

3. Apparatus according to claim 1, belonging to the same home network as said device.

4. Apparatus according to claim 1, belonging to a local network (1) generating said secret information.

5. System for securely storing secret information comprising :

- an apparatus (10 ; 1) containing said secret information ;
- a device meant to use said secret information to decrypt a digital content ;
- a server (20) remote from said apparatus and from said device,

wherein said apparatus (10 ; 1) comprises means for sending said secret information to said server (20) and wherein said server (20) comprises means for storing said secret information.

6. System according to claim 5, wherein said apparatus (10) is part of said device.

7. System according to claim 5, wherein said apparatus (10) and said device are connected to a common home network.

8. System according to claim 5, wherein said apparatus (1) belongs to a local network generating said secret information.

9. Server (20) for securely storing secret information to be used by a device to decrypt a digital content, said device being remote from said server (20),

characterised by means for receiving said secret information through a remote communication.

10. Process for securely storing secret information to be used by a device to decrypt a digital content comprising the steps of :

- initiating a remote communication between an apparatus (10 ; 1) containing said secret information and a server (20) remote from said device ;
- sending said secret information from said apparatus (10 ; 1) to said server (20) ;
- storing said secret information on said server (20).

11. Method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server (20) remote from said device for storing said secret information on said server (20) ;
- providing means (10) for said device to retrieve said secret information from said server (20) and to decrypt the encrypted digital content with said secret information.

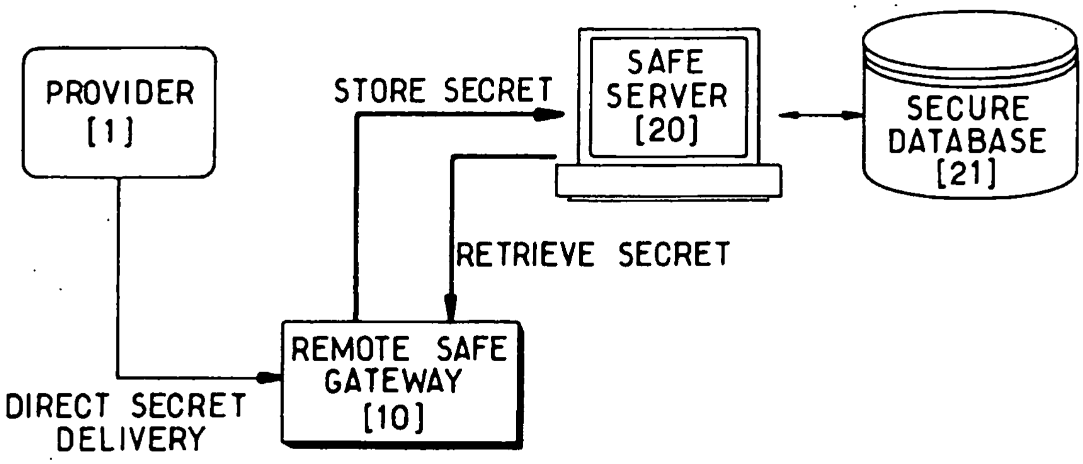

PROVIDER
[1]
STORE SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.1

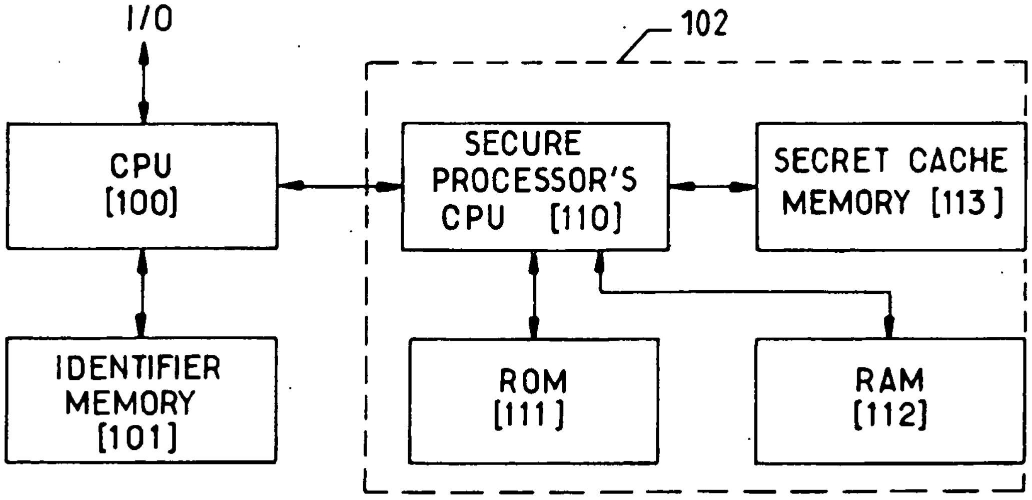

I/O
102
CPU
[100]
SECURE
PROCESSOR'S
CPU [110]
SECRET CACHE
MEMORY [113]
IDENTIFIER
MEMORY
[101]
ROM
[111]
RAM
[112]

FIG.2

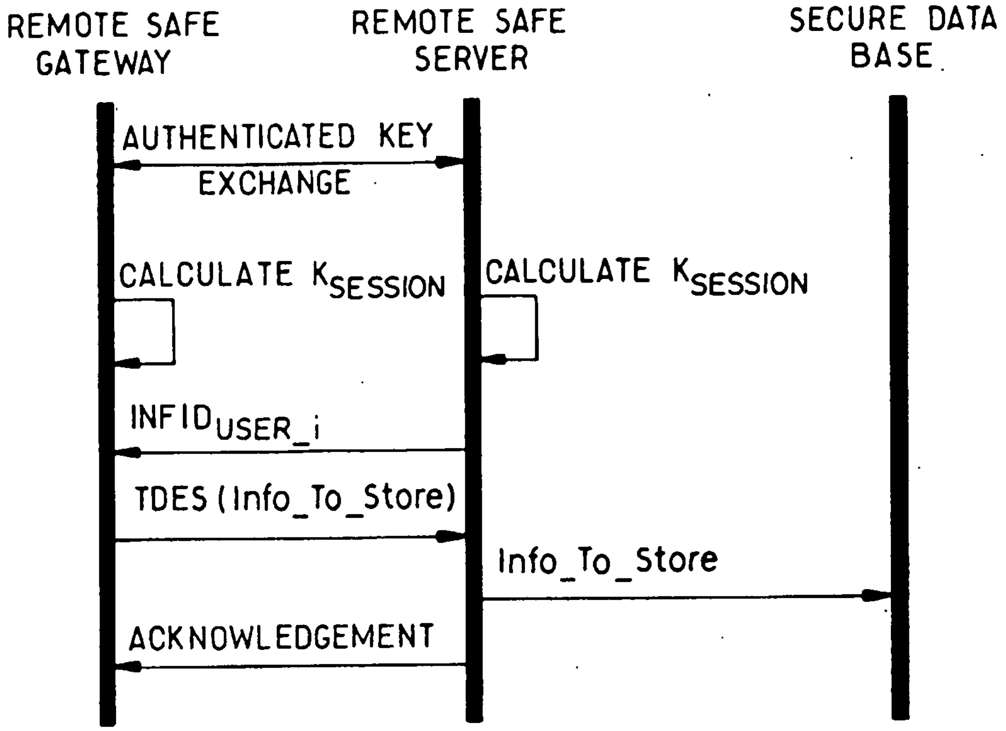

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
TDES (Info_To_Store)
Info_To_Store
ACKNOWLEDGEMENT

FIG.3

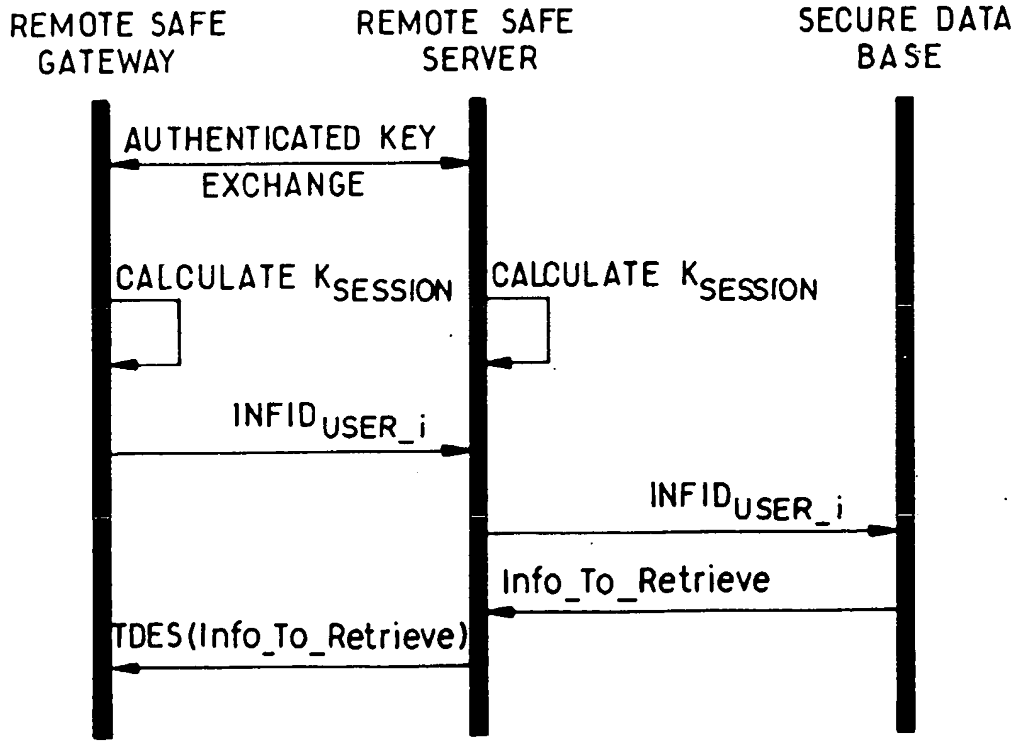

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
$INFID_{USER\_i}$
Info_To_Retrieve
TDES(Info_To_Retrieve)

FIG.4

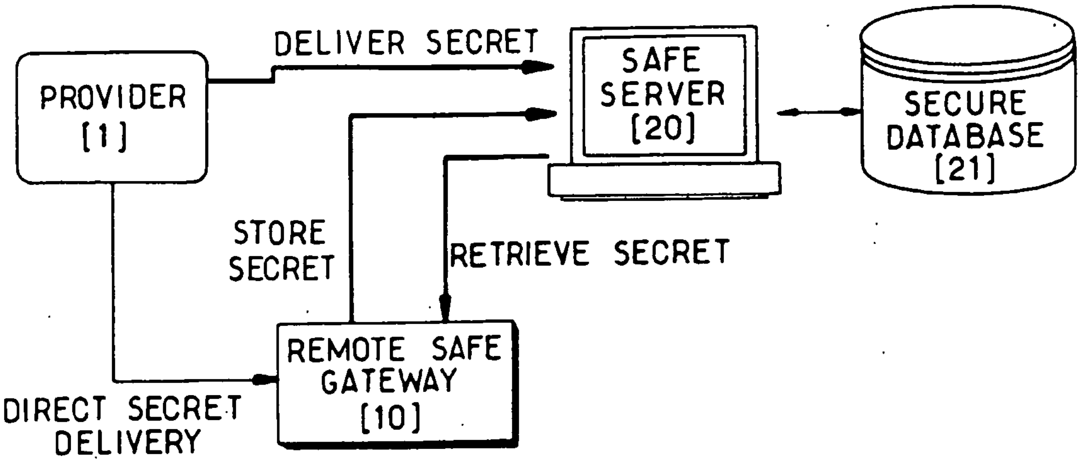

DELIVER SECRET
PROVIDER [1]
SAFE SERVER [20]
SECURE DATABASE [21]
STORE SECRET
RETRIEVE SECRET
REMOTE SAFE GATEWAY [10]
DIRECT SECRET DELIVERY

FIG.5

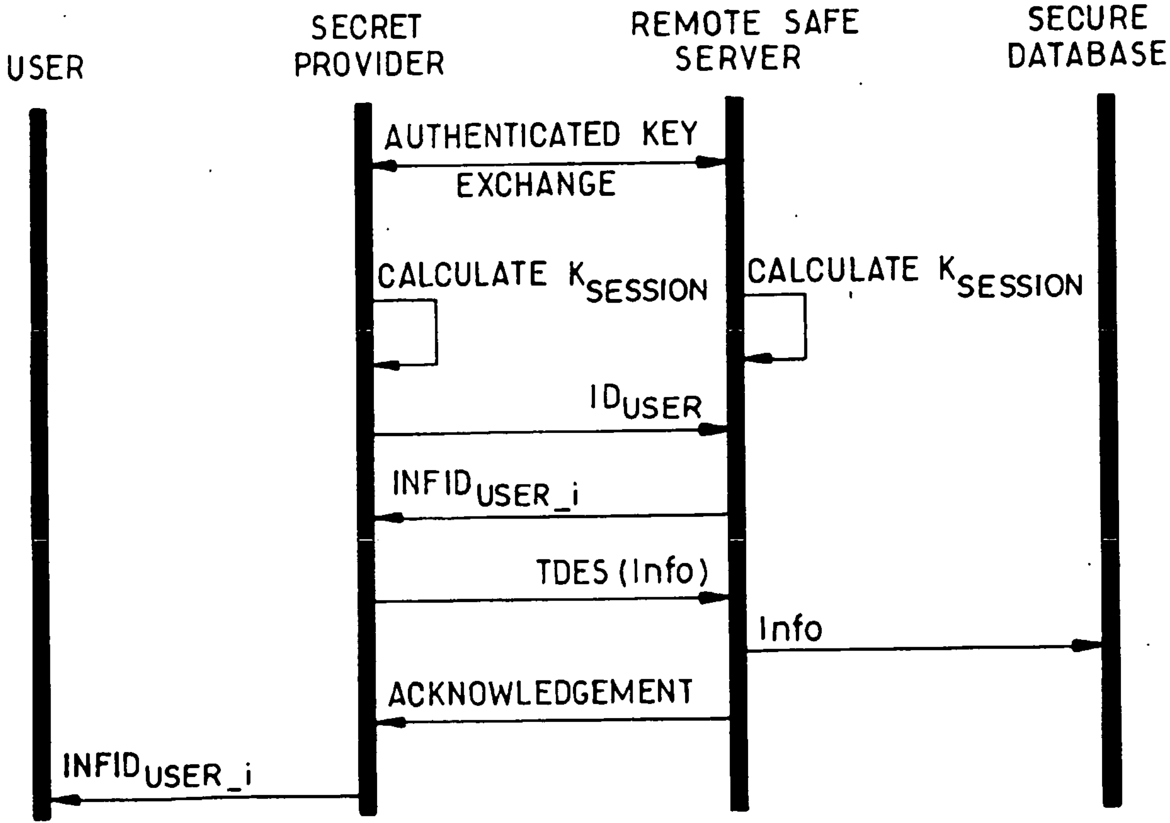

USER
SECRET PROVIDER
REMOTE SAFE SERVER
SECURE DATABASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
ID_{USER}
$INFID_{USER\_i}$
TDES (Info)
Info
ACKNOWLEDGEMENT
$INFID_{USER\_i}$

FIG.6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/04088

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F17/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 337 357 A (CHOU WAYNE W ET AL) 9 August 1994 (1994-08-09) figure 1 column 3, line 26 -column 4, line 37 ---	1-11
X	EP 0 843 449 A (SUNHAWK CORP INC) 20 May 1998 (1998-05-20) column 5, line 8 -column 8, line 19 figures 2-5 ---	1-11
X	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) page 10, line 7 -page 11, line 29 figures 1,5,6,9 -----	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 6 August 2001	Date of mailing of the international search report 14/08/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Papastefanou, E

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/04088

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5337357	A	09-08-1994	CA	2120816	A	18-12-1994
			EP	0636962	A	01-02-1995
EP 0843449	A	20-05-1998	US	5889860	A	30-03-1999
			CA	2220457	A	08-05-1998
			JP	10301904	A	13-11-1998
WO 9842098	A	24-09-1998	AU	6759198	A	12-10-1998
			EP	0968585	A	05-01-2000